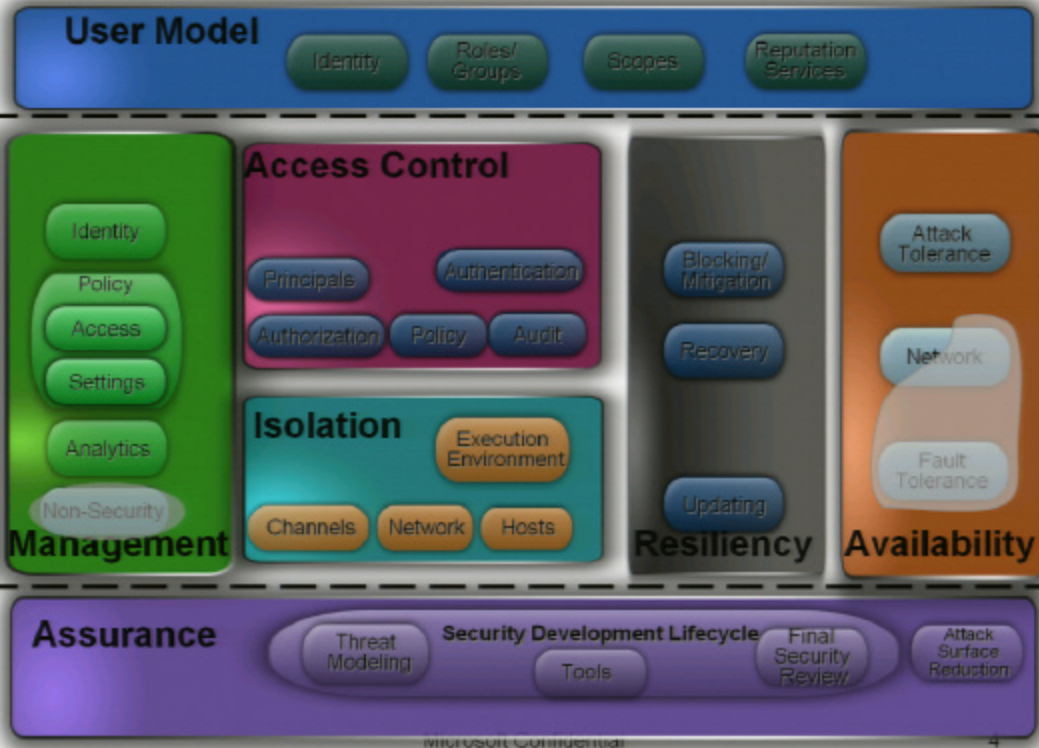
Red|Green

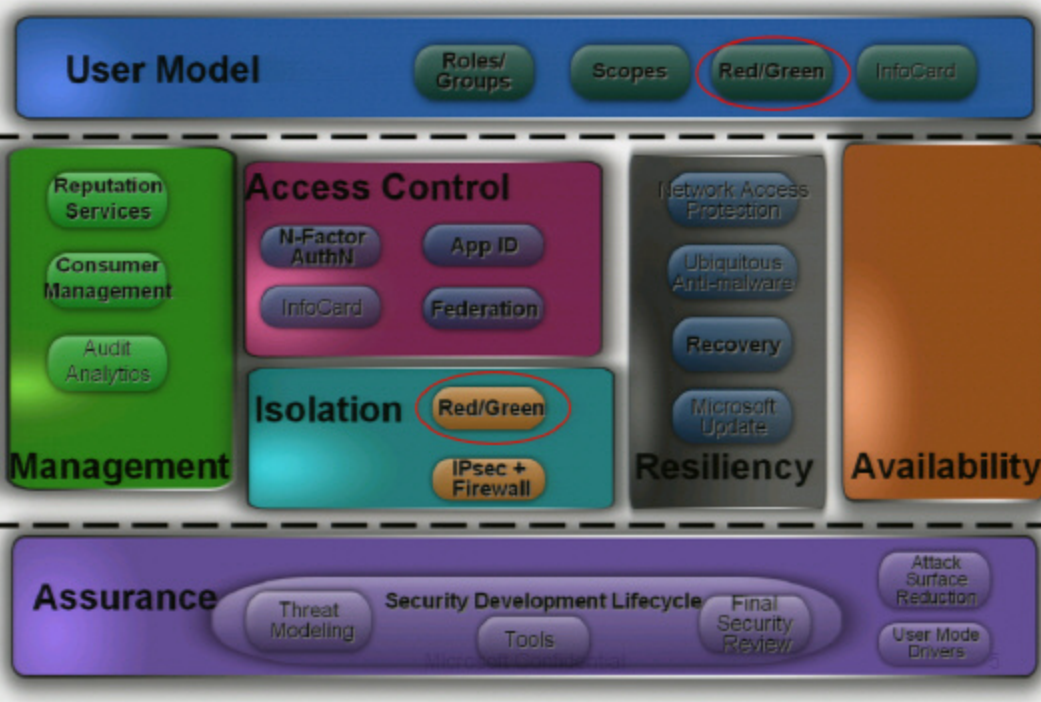
The Red|Green Team
The Zeno Team

Paul England

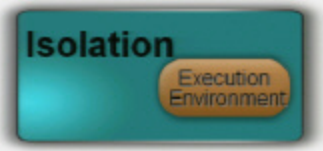
BillG Review – Jul 13 2005


User Model
Identity
Roles/ Groups
Scopes
Reputation Services
Identity
Policy
Access
Settings
Analytics
Non-Security
Management
Access Control
Principals
Authentication
Authorization
Policy
Audit
Isolation
Execution Environment
Channels
Network
Hosts
Blocking/ Mitigation
Recovery
Updating
Resiliency
Attack Tolerance
Network
Fault Tolerance
Availability
Assurance
Threat Modeling
Security Development Lifecycle
Tools
Final Security Review
Attack Surface Reduction

Big Bets


User Model
Roles/ Groups
Scopes
Red/Green
InfoCard
Reputation Services
Consumer Management
Audit Analytics
Management
Access Control
N-Factor AuthN
App ID
InfoCard
Federation
Isolation
Red/Green
IPsec + Firewall
Network Access Protection
Ubiquitous Anti-malware
Recovery
Microsoft Update
Resiliency
Availability
Assurance
Threat Modeling
Security Development Lifecycle
Tools
Final Security Review
Attack Surface Reduction
User Mode Drivers

R|G Defined



- Isolation technology that partitions the world into two parts:
  - Safer/accountable
  - Less safe/unaccountable
- Consists of two, mostly orthogonal, dimensions
  - User Experience—being researched
  - Isolation mechanism—two leading options
    - VM (eventually over the hypervisor)
    - Process isolation with MIC

Red|Green

Paul England

Outline

- Introduction
- Motivation
  - Why VMs?
  - Why Red|Green?
- Red|Green technologies
  - UI/UX
  - Administration
- Discussion topics

What is Red Green?

- VM based client security product
- Mostly about making VM technologies
  - Usable by knowledge workers
  - Easy to deploy and administer
- Building on Virtual Server 2005, XPSP2, RDC
  - Will port to the MS hypervisor when it makes sense
- Hope to ship as a product
- See
  - Dan Simon's "WindowBox"
  - Butler on "Simple Security: Red and Green machines"

How we got here...

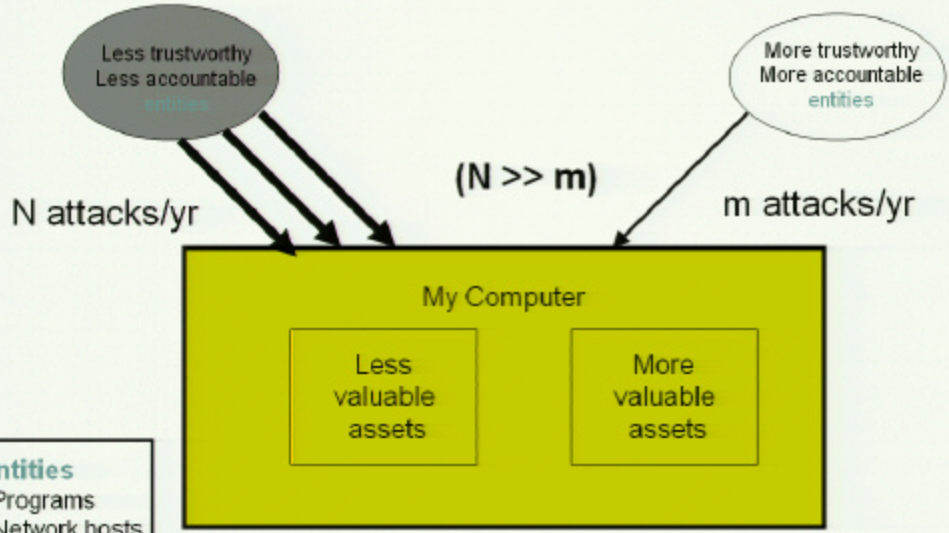
- R|G has always been one of the MS Hypervisor scenarios
  - Hypervisor schedule has slipped
- R|G v1 is "Doing the best we can" with existing virtualization technologies
  - VPC/VS
- Most of the R|G work is independent of virtualization technology

Why Virtual Machines?

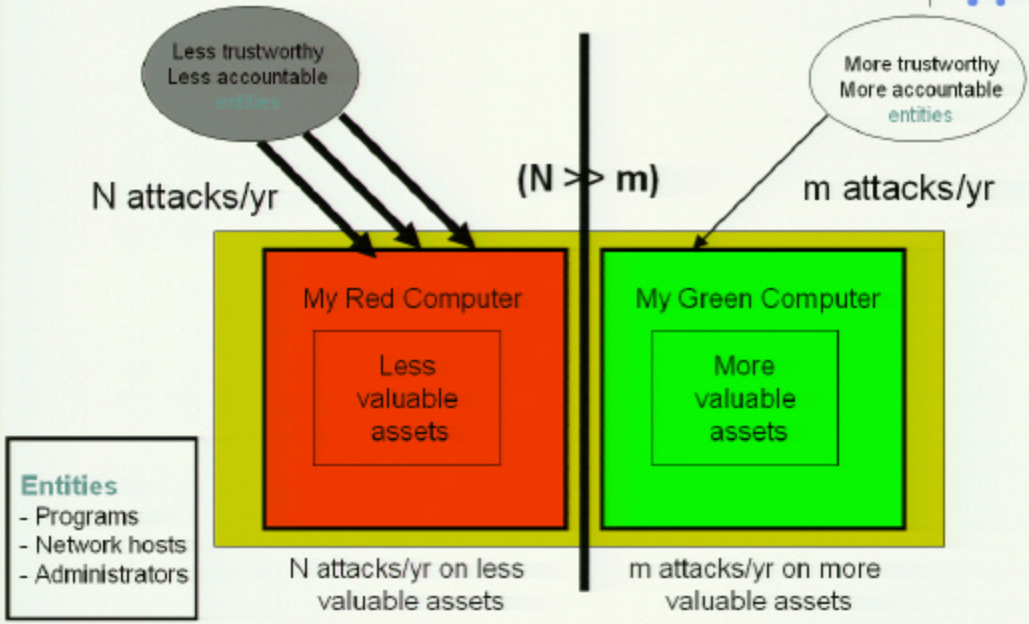
Why Virtual Machines?

- Windows can be configured to be secure
  - Limit interaction with untrustworthy/unaccountable entities
  - An administrator can limit
    - network access
    - the applications that can run
    - Local user admin privileges
    - ..
  - This does not fix the bugs, but makes them benign
  - But this throws away much of the power of the PC
- If you give everyone two PCs, then
  - One can be configured with security first
  - One can be configured with flexibility first
- But this is expensive..
  - So use a VMM...

Without R|G: Today



A Computer with R|G

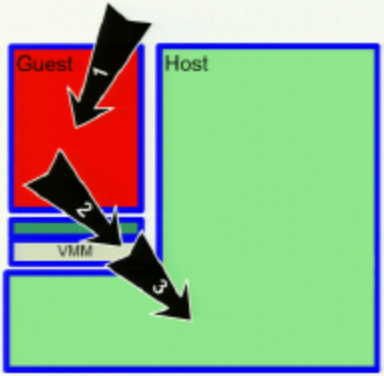


Why Virtual Machines? A slightly different view

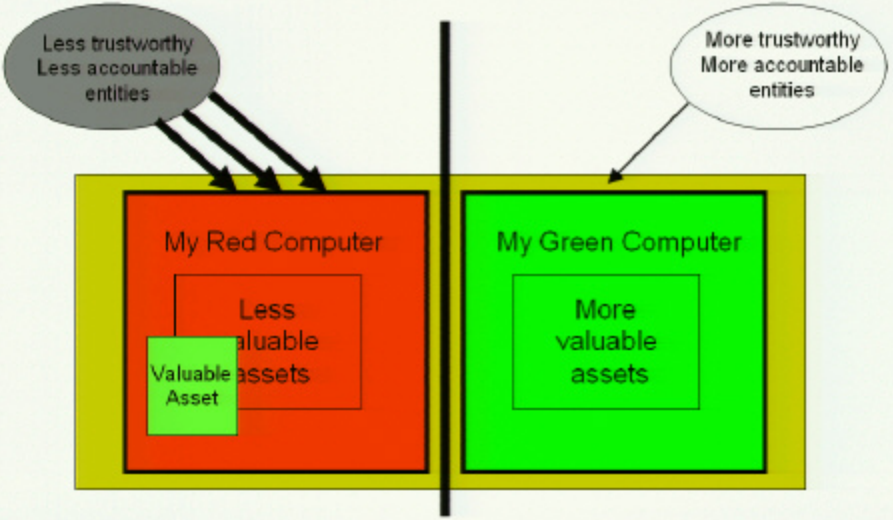
- Windows can't protect itself or user data
  - TCB too big / too many bugs
  - ...Windows process isolation isn't good enough
- And applications are part of the security perimeter
- Use a stronger isolation mechanism
  - separate machines on separate networks?
  - ...but separate machines are expensive and hard to use
- VMMs should provide better isolation

How good is VM-Based Isolation?

- Size of isolation TCB
  - Our VMM is ~ few 100 KLOC
  - The Windows TCB is a lot more
  - VM interface much less complex
    - PC versus Win32
  - Notes
    - Host OS still needs to be secure
    - Including network traffic to guest
- Isolation boundaries are nested
  - Exploiting Green from internet via Red needs simultaneous un-patched bugs in
    - Red (1)
    - the VMM (2),
    - and (sometimes) Green (3)
- But good isolation is only half the story…



Keep valuable stuff out of red



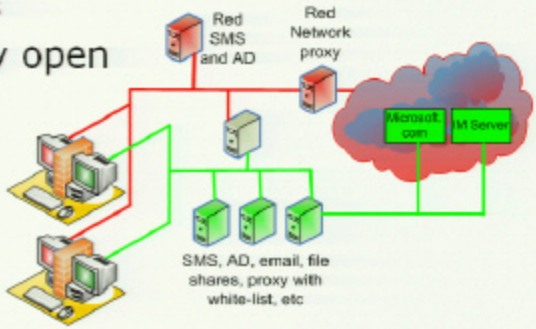
Why Red|Green?

- VMMs can potentially provide qualitative improvements in client security
- But…
  - VS targets server administrators
  - VPC targets developers
- Existing MS VM technologies
  - Using multiple OSs is hard
  - Deploying and administering VMMs and guests is hard
  - Managing multiple OSs is hard (maybe)
- If users & corporations are to benefit from VMs
  - Security
  - Availability
  - Disaster recovery
- We must provide software to mitigate these issues

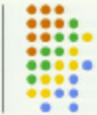
This is the focus of R|G

R|G in the Enterprise: an example

- Green machine–Locked down
  - Software restriction policies …
  - Connects to CorpNet
  - No local user admin privs
- Red machine–Relatively open
  - Run any program
  - Connects to internet
  - Local user is admin



Why Red|Green?

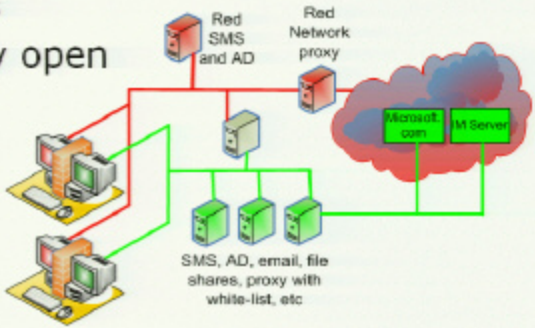


- VMMs can potentially provide qualitative improvements in client security
- But…
  - VS targets server administrators
  - VPC targets developers
- Existing MS VM technologies
  - Using multiple OSs is hard
  - Deploying and administering VMMs and guests is hard
  - Managing multiple OSs is hard (maybe)
- If users & corporations are to benefit from VMs
  - Security
  - Availability
  - Disaster recovery
- We must provide software to mitigate these issues

This is the focus of R|G

R|G in the Enterprise: an example

- Green machine–Locked down
  - Software restriction policies …
  - Connects to CorpNet
  - No local user admin privs
- Red machine–Relatively open
  - Run any program
  - Connects to internet
  - Local user is admin



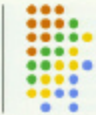
Characteristics of simple enterprise R|G scenario

- Corporate email, servers, etc. available in green
  - Most important corporate data will be created, processed, saved,… on green machines and networks
- Some important data is collected in red
  - Some will stay in red:
    - Cookies, favorites, acrobat reader …
  - But if data is to be incorporated into enterprise docs
    - It will have to be copied into green
- For most enterprises, with simple R|G internet/intranet net partitioning
  - Good data in green
  - Unimportant data in red
  - Bad code in red

Target Customers / Scenarios

- We are shooting for enterprise / corporate
  - E.g. simple R|G scenario above
- How about the home?
  - Safe place for IE, peer-peer, chat
- Issues
  - Performance of guest OSs
    - Red performance acceptable for: Home? Office?
  - Guest virtual hardware availability
  - Corp role separation easier to understand / enforce
  - User confusion:
    - where are my pictures? Where should they be?
    - I just installed a picture viewer application - it doesn't work
    - ...
  - Ichiro "is on our side" in an enterprise

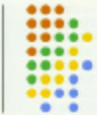
Marketing Red Green (an engineers view)



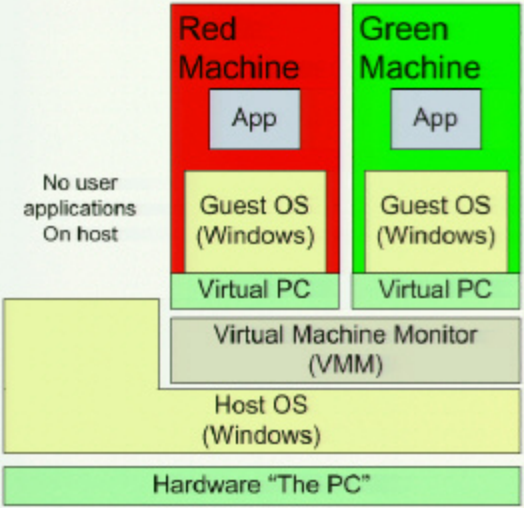
- End user view
  - Security gets in the way
    - V1 Red/Green will get in the way
    - …Hard to market to end users
- Ichiro's view
  - He gets to make uncompromised net and OS configuration choices for green
  - Green machine and green net compromise less likely
  - Red flatten / rebuild is free
- For an enterprise we hope R|G will
  - Reduce support costs
  - Increase net/machine availability
  - Increase corporate data security
    - Detailed analysis in progress
- Note: the techies like lots of VMs for specialized purposes
  - Will support this, but not the focus of the R|G project

VM Platform Technologies

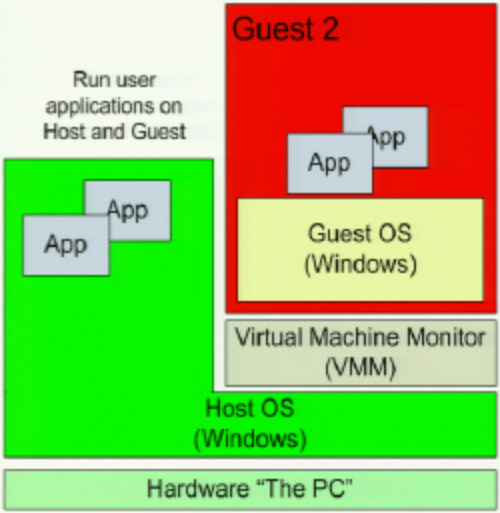
R|G on a Hosted VMM



Option I: Red and Green Guests

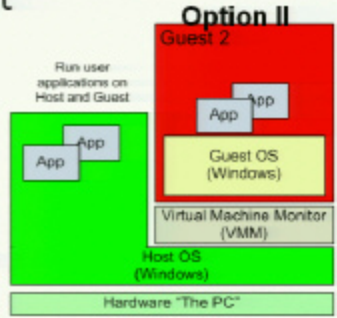


Option II: Green Host, Red Guest



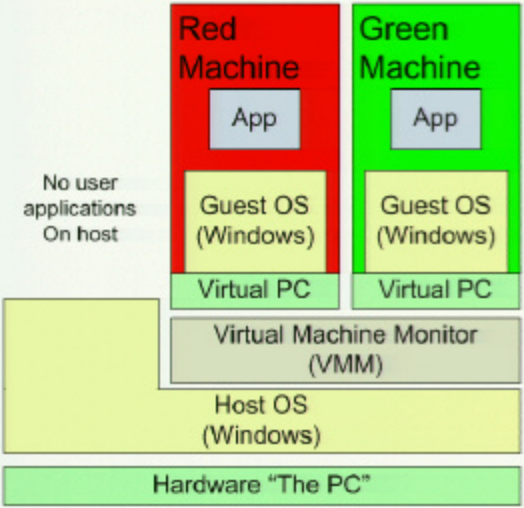
VMM Issues

- Guest is not as good as the host
  - Only a few I/O devices available
  - Poor performance – particularly video
- Most administrators will opt for
  - Green host
  - Red guest or guests
- An administrator could..
  - Lock down the host
  - Have red and green guests
    - But we don't think that they will...
  - Will target this for "typhon"

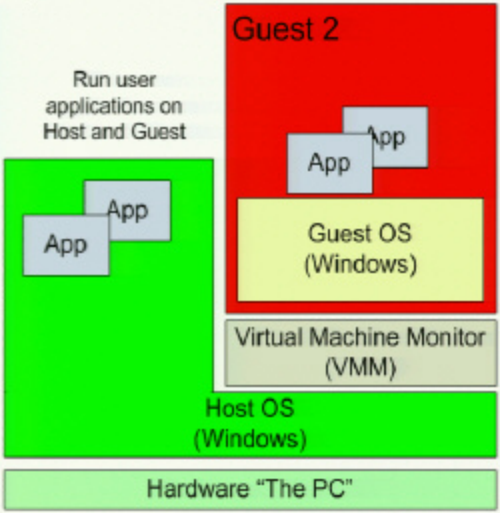


R|G on a Hosted VMM

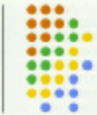
Option I: Red and Green Guests



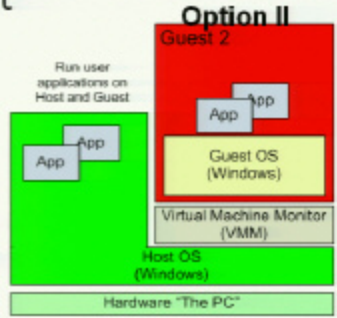
Option II: Green Host, Red Guest



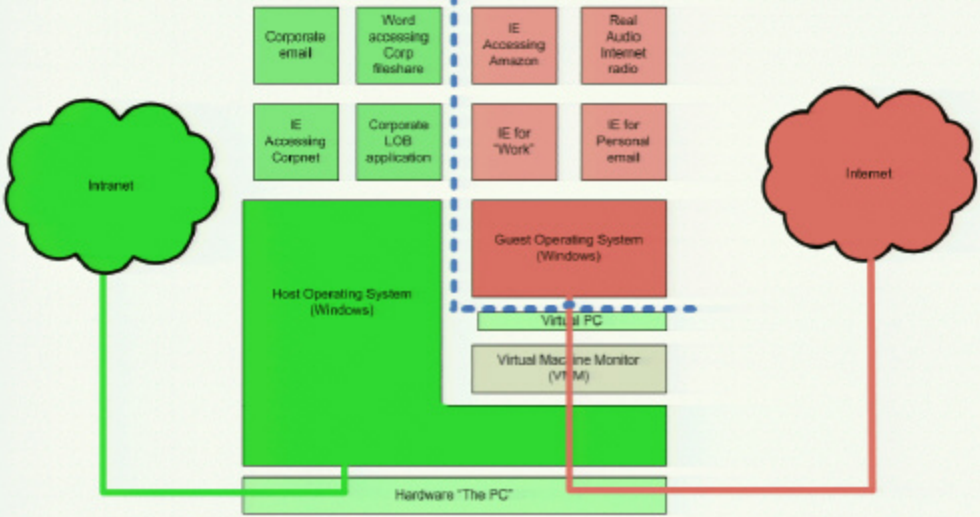
VMM Issues



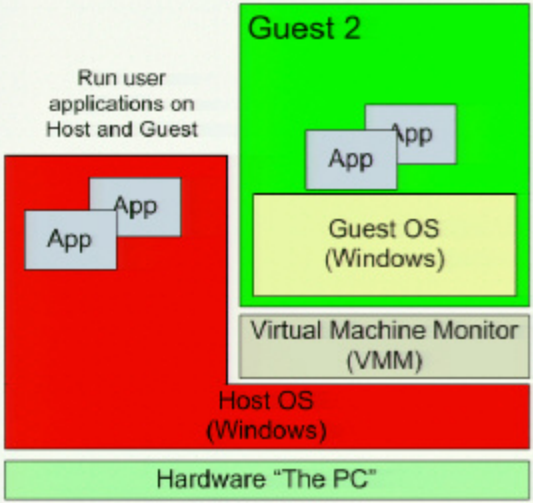
- Guest is not as good as the host
  - Only a few I/O devices available
  - Poor performance – particularly video
- Most administrators will opt for
  - Green host
  - Red guest or guests
- An administrator could..
  - Lock down the host
  - Have red and green guests
    - But we don't think that they will...
  - Will target this for "typhon"



Typical Configuration

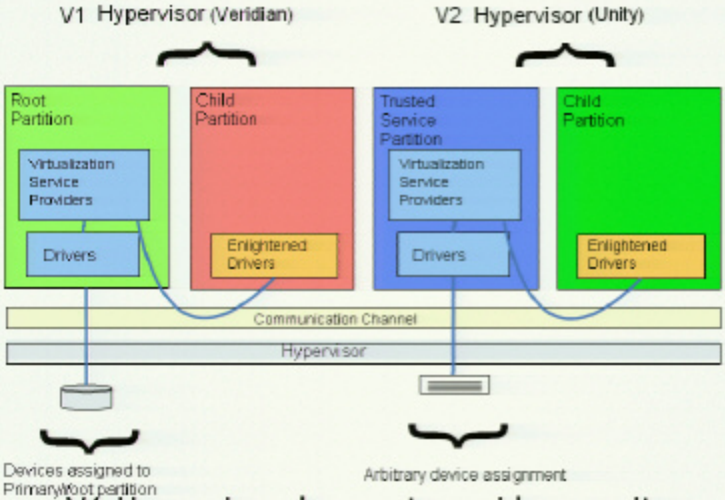


Red Host - No Good for R|G



- Might like this so that games can run in red
- But all guests must trust the host
- Malware in the host can observe and modify any aspect of guest behavior
- We can start to do things like this with the hypervisor

Hypervisor



- V1 Hypervisor does not provide security benefits
- V2 hypervisor may

R|G Technologies and User Model

Why not just use VPC?

- VPC/VS are designed for
  - Server consolidation
  - Developers
- We are trying to make VM technologies
  - Usable by knowledge workers
  - Deployable by system administrators
- We must improve VPC/VS
  - Security, Usability, Deployability, Serviceability, Manageability
- **This is the focus of R|G**

R|G Platform (what we are building upon)

- VS 2005
  - (possibly de-featured)
  - Newer code base than VPC
  - Better programming interface than VPC
- Remote desktop AX control for UI
  - More programmable than VPC / emulated S3
    - E.g. Can do single-sign-on, integrate into our UI framework
  - Better forward path to support RAIL
  - Better support for sound, smartcards, etc.
  - Attack surface is an issue
- XPSP2

RG Technologies

- The GuestBar
  - Switching machine focus / window management
  - VM & VMM admin
  - Alert forwarding
- Single sign on / single machine
  - E.g. Windows-L does something sensible
  - Seamless logon
- The Airlock
  - Securable inter-guest communication
  - Including cut/paste, drag/drop, etc.
- "Enlightenments"
  - Moving files and setting
  - Make IE, shell work better in multi-OS environment
- Administration Support Technologies
  - Guest manager / database
    - Mapping VMM name to guest DNS name, etc. Remote administration
    - WMI wrappers
  - Deployment
  - Tools, utilities

R|G User Model Dilemma

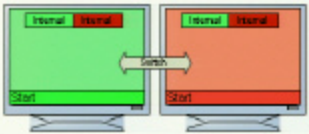
- People don't want complete isolation
  - They want to:
    - Cut/paste, drag/drop
    - Share parts of the file system
    - Share the screen
    - Administer one machine, not two
    - …
- But more integration can weaken isolation
  - Add bugs
  - Compromise security
- To find the right balance we must
  - Usability test
  - Dog-food
  - Run betas

Screen Sharing Models

- How does the user interact with the red, green, orange… machines…
  - "KVM switch" (full screen switcher)
  - Fully integrated (X-Windows / RAIL)
  - Recursive desktop (RDC, VPC)

Sharing the Screen - Choices

- Switched desktops (virtual KVM)



Virtual KVM

- Multiple desktops on the screen at the same time
  - Recursive desktops
  - Tiled desktops

Recursive Desktop

- Single desktop, composited application windows

Fully Composited Desktop

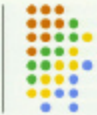
Screen Sharing Issues

- Issues:
  - User confusion
    - Doing the right thing in the right environment
  - Spoofing
    - Phishing
  - How separated are user activities?
- Solution:
  - Lots of dogfooding
  - Lots of usability testing
    - Already done usability on virtual KVM
      - Tests well, but we will prototype other models too

UI Plan

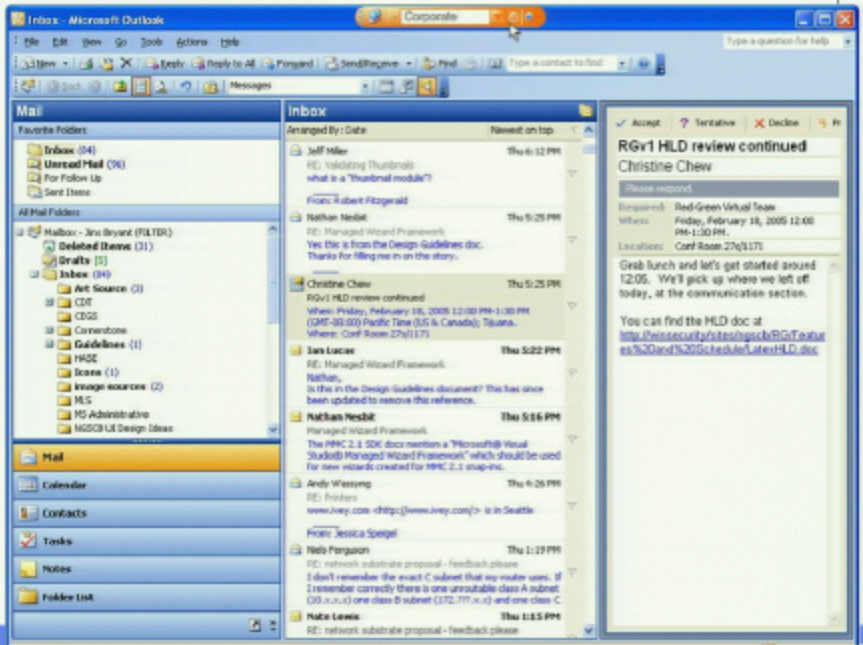
- What we can do today…
  - Full screen switch
  - Recursive desktop
  - Can do recursive desktop on Longhorn
- Usability studies heavily favor full screen switch over recursive
- We will
  - Optimize for full screen
  - How important is side-by-side?

GuestBar Prototypes

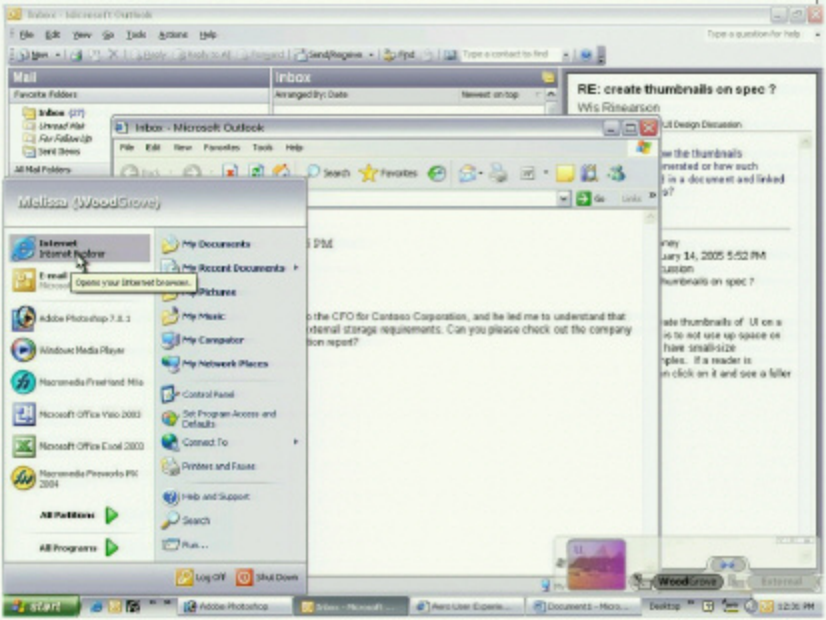


- The GuestBar is the desktop switcher
- Prototypes
  - Docking auto-hiding toolbar
  - Integrated with existing taskbar
  - Floating, non intrusive, always-on-top application

Floating Desktop Switcher



Taskbar integrated



Airlock (Data Transfer)

- Mediates data transfer between machines
  - Drag / drop, Cut / paste, Shared folders
- Issues
  - Red → Green: Malware entering (integrity)
  - Green → Red : Information leaking (confidentiality)
- Policy
  - Allowed transfers (configurable). Examples
    - No transfer of ".exe" from R to G
    - Only transfer ASCII text from R to G
    - Transfer rich-text format between environments, no macros
  - Non-spoofable user intent
  - warning dialogs
  - Auditing
  - synchronous virus checker
  - attachment execution services (AES) check
  - Third party plugin hooks

Shared File System

- Could share any folder or folders
- Possible default configuration
  - Only shared folder is "My Airlock"
  - Subject to airlock policy
- Security policy application
  - Airlock policy
  - OS policy
    - Green examples
      - E.g. Software Restriction Policy limits applications that can run
      - E.g. Word policy forbids unsigned macros

Single Sign On / Single Machine

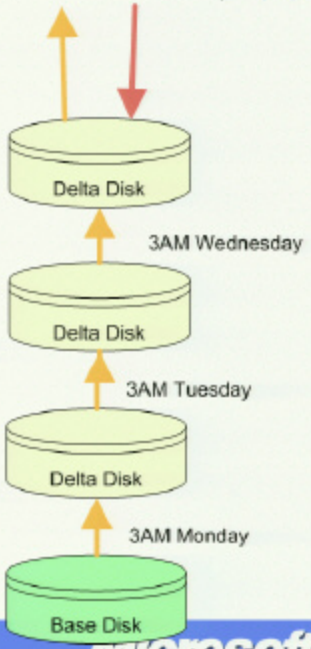
- Single sign on
  - Constrained by RDC and XPSP2
  - We can cache red password in green
    - Encourage different user accounts in R and G
- Single machine
  - Constrained by RDC behavior
    - It looks pretty good…
  - And since RDC is a Web download, we might be able to fix stuff
  - But some user confusion is inevitable…

Other User Experience Issues

- Click on a data file, URL, etc, "do the right thing"
  - Simple examples
    - "Intranet" URLs open in green
    - "Internet" URLs open in red (except trusted sites)
  - Harder examples
    - Opening documents with macros
- Single administration of all environments
- …
- Big challenge is balancing:
  - Convenience
  - User confusion
  - App Compatibility

VM Resiliency Support

- VS has features for disk snapshot and rollback
- Malware attack
  - Roll machine back to yesterday
- Other admin possibilities
  - Each machine gets a pristine, up-to-date OS every day
- Investigation:
  - Can some state be preserved during rollback?



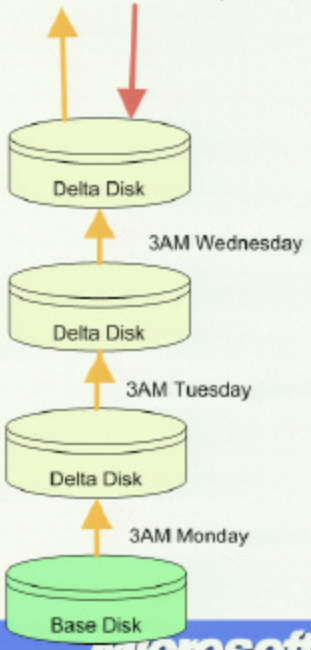
Other User Experience Issues

- Click on a data file, URL, etc, "do the right thing"
  - Simple examples
    - "Intranet" URLs open in green
    - "Internet" URLs open in red (except trusted sites)
  - Harder examples
    - Opening documents with macros
- Single administration of all environments
- …
- Big challenge is balancing:
  - Convenience
  - User confusion
  - App Compatibility

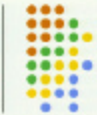
Other Issues

VM Resiliency Support

- VS has features for disk snapshot and rollback
- Malware attack
  - Roll machine back to yesterday
- Other admin possibilities
  - Each machine gets a pristine, up-to-date OS every day
- Investigation:
  - Can some state be preserved during rollback?



R|G Administration

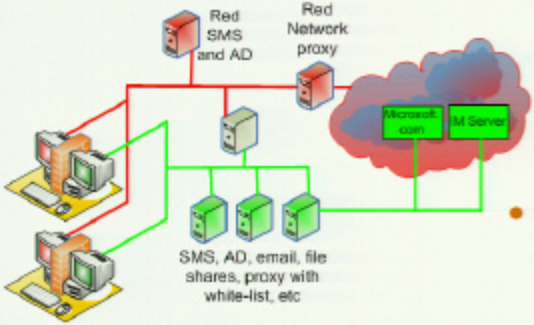


- Basis: administered exactly as they are today
  - Then tweak – e.g.
    - Virtual machine enumeration
    - Host to guest mapping
    - Programmatic guest install, start, rollback
    - Server tools and utilities
- Cost to manage twice as many OSes?
  - – SMS etc. scale well with number of OSes
  - – Fewer Green compromises with R|G
  - – Red compromises not very important, quick to fix
  - + Two different machine profiles
- Need client and server tools to reduce costs

Patching

- You patch twice!
- Some mitigating issues
  - Many enterprise customers are switching on Windows Update
    - This may be more feasible in an environment with VMs
    - Patching Green is less urgent when Ichiro can configure for security

R|G and Enterprise Networks



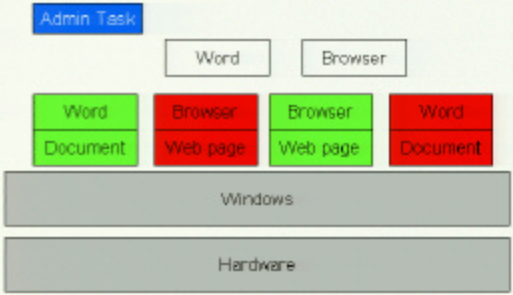
- red and green networks are defined as today:
  - IPSEC
  - NAP
  - guest firewall
  - proxy settings
  - …
- the VMM helps by doing things that could previously only be done in the network
  - E.g. red only talks to the proxy
  - Soft port shutdows

Red|Green Inside Windows?

Process Isolation: R|G inside Windows

- Session isolation

- Mandatory Integrity Control (MIC) isolation
  - Each process in the session runs at the level of the object



R|G using MIC

- Implementation: R runs at lower MIC level, objects labeled R or G
  - Default access rules:
    - R can't modify G; R can't read G
    - G won't execute R binaries (.exe, .dll, etc.)
    - R can execute G binaries
  - Objects automatically labeled R or G when created
    - G process creates G objects; R process creates R objects
    - No constraints on file location
  - AES handles files that arrive from "outside"
    - Could cause G process to mark file as R
  - Apps launch at level of file (ShellExecute)
    - Apps could be R|G aware and change behavior slightly
      - E.g. Word mightn't run macros in R files
  - "Airlock" to change files from R to G
- UI: Windows (with R/G chrome)
  - Shell shows color of file

Isolation Technology Trade-Offs

	Pros	Cons

VMM	• High assurance isolation
	  • Small, well understood boundary
	• Simple snapshot/rollback of red
	• Defense in depth
	  • VM + user/kernel + session,
	• App compatibility
	• "Big" pieces exist today
	• Red users can be admin
		• Guest graphics performance
		• Guest device availability
		• Extra OS to administer
		• Lots of work to integrate R|G "well"

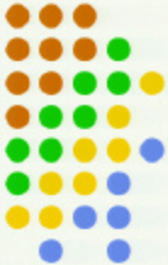
Process: MIC	• Only one OS to administer • Extension of LH MIC (e.g. LRIE) • Fast graphics in Red • Simpler for safe browsing, email, IM • Same user profile in R, G	• Lower assurance isolation • Red user can't be admin • Other app compat issues • Can't install kernel drivers
Process: Session	• Only one OS to administer • Fast graphics with KVM • Device availability on Red	• Lower assurance isolation • Red user can't be admin • Other app compat issues • Slow graphics on shared screen

A few things to think about

R|G using MIC

- Implementation: R runs at lower MIC level, objects labeled R or G
  - Default access rules:
    - R can't modify G; R can't read G
    - G won't execute R binaries (.exe, .dll, etc.)
    - R can execute G binaries
  - Objects automatically labeled R or G when created
    - G process creates G objects; R process creates R objects
    - No constraints on file location
  - AES handles files that arrive from "outside"
    - Could cause G process to mark file as R
  - Apps launch at level of file (ShellExecute)
    - Apps could be R|G aware and change behavior slightly
      - E.g. Word mightn't run macros in R files
  - "Airlock" to change files from R to G
- UI: Windows (with R/G chrome)
  - Shell shows color of file

A few things to think about



R|G in the home

- Consumer is harder than enterprise
  - Poorly defined boundaries
    - Safe / unsafe is harder to define
  - Administration
    - Consumers don't have real management (yet)
- Most of enterprise is needed for consumer
  - Very few things aren't needed (e.g. AD)
- Solutions
  - Extend R|G V.2 to provide consumer support
  - Build a consumer security administration eco-system
    - Extend OneCare to provide consumer security administration

How interesting is rollback?

- It is easy to
  - automate guest disk checkpoint / snapshot
  - Provide users/admin ability to roll back
- Can we do more?
- Issues
  - We already have 2 or 3 Windows-based roll back technologies
  - Guest perf likely forces most interesting data to be on the host
    - …And the VMM can't roll back the host
- Options
  - For v1: Do it, but only at disk level
  - Grope around in guest disk (FSTW, etc.) (v.next?)
    - roll back some data
    - preserve other data